ALERT LOGIC™

CASE STUDY

Big Projects, Big Challenges

Securing The Future With Alert Logic

Bentley's solutions are used to design, build, and operate roadways, bridges, airports, skyscrapers, and industrial plants across the globe. They are adapted to meet the unique demands of each individual project; be it a 50-story office tower in the heart of London, the world's largest crude oil refinery in India, or the iconic main terminal building at Abu Dhabi airport.

The company's services bring benefit to the legions of engineers, architects, planners, contractors, IT managers, and operators involved in each project for its entire lifetime, and all projects are supported by its worldwide Professional Services organization.

The Challenge

The high-profile nature of many of Bentley's clients' projects dictates that security and data integrity are always major considerations. Tom Cibelli, Solutions Engineering Manager for Bentley Systems, elaborated, "One of the first questions we always get asked by new clients is about the security of our systems and the data we're managing for them. Without a compelling response, these discussions can quickly get very involved and ultimately impact the length of the sales cycle, which of course nobody wants."

Bentley® Advancing Infrastructure

ABOUT

Customer: Bentley Systems

Industry: Computer Software

Location: Pennsylvania, US

SOLUTIONS

- Alert Logic® Threat Manager™ with Alert Logic® ActiveWatch™ – combines a cloud-based intrusion detection system (IDS) and vulnerability assessment solution – delivered as a service that works in any datacenter environment, from on-premises to the cloud.
- Alert Logic® Log Manager™ with Alert Logic® ActiveWatch™ – increases visibility, rapid custom reporting, and scalable, real-time log collection and management for any datacenter environment.

One of the steps taken by Bentley to address this situation has been to attain compliance with key industry standards, including the stringent ISO 27001 information security mandate. "With it recognized globally and administered by an objective third-party, being able to state we're compliant with ISO 27001 removes a lot of the concerns. However, in order to continually meet the requirements we needed to implement the right set of security controls," noted Cibelli.

The sophistication and sheer scale of Bentley's solutions imposes significant demands on any component deployed in its IT infrastructure. Cibelli explained, "We customize a large number of our implementations and are constantly innovating: We have to ensure that the technology choices we're making don't restrict us doing so. Scalability, flexibility, and the ability to perform across a diverse set of environments are all critical selection criteria for us."

As part of the process to attain ISO 27001 compliance, Cibelli and his team needed to identify solutions to handle intrusion detection, vulnerability assessments, and real-time log file collection and management. With an ongoing commitment to transition more of its services into the cloud, it was imperative for Bentley that the security solutions would perform with both on-premise and cloud-based deployments.

"What really stood out from the competition was that it was clearly evident that Alert Logic was very familiar with a broad range of standards – including ISO 27001 and Sarbanes-Oxley – the team really understood what was involved in satisfying the most rigorous industry requirements."

TOM CIBELLI,
SOLUTIONS ENGINEERING MANAGER FOR BENTLEY SYSTEMS

Why Alert Logic?

Cibelli already had familiarity with the Alert Logic portfolio through Bentley's own private cloud vendor that provided infrastructure-as-a-service capabilities from its managed data center. He recounted, "With our firsthand knowledge and positive experiences, when we needed to implement the same functionality ourselves, Alert Logic automatically made the short list."

After an extensive discovery and evaluation process, Bentley purchased Alert Logic® Threat Manager™ and Alert Logic® Log Manager™, both with Alert Logic® ActiveWatch™ to provide additional expertise for the company to call on.

When Cibelli started the roll-out process, Bentley was using a combination of Microsoft Azure, Amazon Web Services, as well as the regional cloud provider to deliver its cloud-based services. The ability for Alert Logic appliances to work in each of those environments was a major benefit. He reflected, "What really stood out from the competition was that it was clearly evident that Alert Logic was very familiar with a broad range of standards – including ISO 27001 and Sarbanes-Oxley – the team really understood what was involved in satisfying the most rigorous industry requirements."

The Results

Implementation of the Alert Logic solutions brought immediate benefit by contributing to Bentley's ISO 27001 certification. "This in turn contributes significantly to the comfort levels of both our existing users with our security policies, as well as new customers coming onboard with our managed services," stated Cibelli.

Bentley uses Alert Logic intrusion detection capabilities to monitor traffic across its managed services environments and information is transmitted directly to Alert Logic data centers. Events are monitored by the team of ActiveWatch security experts and notifications are generated for any suspicious activities. If necessary, impacted systems are identified and a remediation strategy is immediately tailored to address the issue. "Incident response procedures are a key requirement for our ISO 27001 compliance, and they all tie back to Alert Logic," commented Cibelli.

Threat Manager gives Cibelli the ability to do an in-depth analysis of potentially malicious events. He noted, "Because I can pinpoint the origin of any suspicious traffic, I even use the information to inform other companies that they might have a problem with their own servers."

Log Manager enables logs to be extracted for immediate transportation to a third-party location that isn't affiliated with Bentley. "This is really important for us," stated Cibelli, "Our people don't have direct access to be able to modify log files. Should there ever be a security incident, we can prove that we haven't manipulated any records." If needed, forensic investigations can be performed on retained files to determine root causes of any potentially malicious activities.

Cibelli concluded, "Alert Logic has enabled us to protect datacenters in our multi-cloud environment and we appreciate the security continuity we receive from Alert Logic as we move all-in on Azure.

We've enhanced our overall security posture while leveraging the Alert Logic name with our prospects: People are familiar with the Alert Logic brand and what it represents, and this gives us the instant credibility that we're using best-in-class components to empower our solutions."